Cyber Warfare: does International Humanitarian Law apply?

International Committee of the Red Cross ⋮ 9-11 minutes ⋮ 2/15/2021

You don't need to be a cybersecurity expert to see that in today's highly interconnected and digitally dependent societies, anything with an Internet interface is vulnerable to cyber threats from anywhere in the world.

We're asking an ICRC expert on cyber warfare and international humanitarian law, Tilman Rodenhäuser, to unpack for us what is at stake in the current peak in intergovernmental discussions on existing and potential threats in cyberspace, how applying international humanitarian law – also referred to as the laws of war or law of armed conflict - to military cyber operations can help avert the significant threats they pose to civilians, and why cyber questions concern all States.

1. Why are military cyber operations a humanitarian concern?

Cyber-attacks and their consequences are on top of the agenda around the world. The concern for us, as a humanitarian organization, is that military cyber operations are also becoming part of today's armed conflicts and can disrupt the functioning of critical infrastructure and vital services to the civilian population.

For example, healthcare systems are increasingly digitalized and connected but often unprotected, therefore particularly vulnerable to cyber-attacks. Too often, in armed conflict water and power infrastructure, or hospitals, are damaged by shelling and services are functioning only partially if at all: imagine a major cyber incident on top of it! This can have devastating consequences. Civilians caught in conflict and violence are already struggling enough as it is to see their hardships worsen.

We are also increasingly relying on new and digital technologies to support humanitarian programs, for instance by capturing and using information to inform and adjust responses or by facilitating two-way communication between humanitarian staff and civilians affected by conflict or violence. But this, too, makes us vulnerable to cyber operations that could impact our capacity to protect and assist during humanitarian emergencies.

We also see an increasing risk of intentional and unintentional harm to affected populations, notably through the (mis)use of data by warring parties and or the spread of misinformation, disinformation, and hate speech.

While few States have acknowledged publicly that they have used cyber means in support of their military operations, it is estimated that more than 100 States have developed—or are developing—military cyber capacities. Fortunately, cyber operations during armed conflicts do not occur in a legal vacuum: they are governed by international humanitarian law (IHL).

2. Almost daily we hear about 'cyber-attacks'. When does international humanitarian law apply to such operations?

There are indeed countless cyber operations happening every day, from cybercrime, to cyber espionage, to what many refer to as 'State-sponsored operations'. To most of them, IHL does not apply: IHL applies only to cyber operations that are conducted in the context of an armed conflict.

Admittedly, the question of whether IHL applies to cyber operations is a point of contention in the ongoing UN-mandated cyber processes. But the issue is less controversial when we speak to practitioners. Here, hardly anyone disputes that IHL applies to cyber operations during armed conflict.

Saying otherwise would result in an absurd situation where attacking a hospital with a missile would be prohibited by IHL, but this prohibition would not protect the computers, medical devices, and networks of the same hospital against the dangers of cyber-attack.

In our views, the law is clear on the matter: IHL limits cyber operations during armed conflicts just as it limits the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.

This view has also been taken by the International Court of Justice.

A more complex question is whether a cyber operation can itself trigger the application of IHL. Regarding international armed conflicts, the consensus is that 'an armed conflict exists whenever there is a resort to armed force between States'. But when is this point reached in situations involving cyber operations that do not physically destroy or damage military or civilian infrastructure? That remains unclear.

3. Doesn't 'cyber warfare' only concern technologically advanced States?

It does not and it should not. Cyberspace is highly interconnected by nature. As such, attacks carried out in cyberspace against one State can affect many others, deliberately or incidentally, wherever they are located.

We saw this dynamic in recent years, when malware spread quickly and left hardly any country unaffected, freezing government agencies, paralyzing corporations and crippling logistics centers, costing billions in losses and fixes. In times of armed conflict, these indiscriminate and global effects of military cyber operations can be avoided, or at least limited, if IHL is respected.

Effectively regulating cyber operations during armed conflict is thus of concern for all States, whatever their level of technological development, their military cyber capabilities, or their involvement in armed conflicts.

Get the latest news and updates about our work.

4. Is existing international humanitarian law adequate and sufficient to apply in cyberspace, or is a new cyber convention needed?

One of the great strengths of international humanitarian law is – as pointed out by the International Court of Justice – that it is designed in such ways that it applies 'to all forms of warfare and to all kinds of weapons', including 'those of the future'.

The basic rules are straightforward: targeting civilians and civilian objects is forbidden; indiscriminate weapons and attacks must not be used; disproportionate attacks are prohibited; medical services must be respected and protected.

The same rules and principles – including the principles of humanity, military necessity, distinction, proportionality and precautions – apply to all military operations, be they kinetic or cyber, and must be respected.

However, there are questions that remain highly debated among States and other experts and need clarification. For example, there is disagreement whether civilian data – which are unique to cyberspace – enjoy the same protection as civilian objects. Such disagreements on legal interpretations have always existed without questioning the applicability of the law as such.

Deciding whether a new convention is needed for cyberspace reaches far beyond the use of cyber operations during armed conflicts: it concerns a much larger spectrum of international law issues.

In our view, should new rules be developed to regulate cyber operations during armed conflict, they must build on and strengthen the existing legal framework, in particular IHL. And until any additional

rules are developed, any cyber operations during armed conflict must comply with existing rules of IHL.

5. Does international humanitarian law legitimize the militarization of cyberspace or cyber warfare?

No. Affirming that international humanitarian law applies to cyber operations during armed conflicts does not legitimize cyber warfare, just as IHL does not legitimize any of the other forms of warfare.

In fact, this fear about a possible legitimization of warfare was repeatedly raised in intergovernmental discussions. But States addressed such a fear in 1977 by stating – in the preamble to First Additional Protocol to the 1949 Geneva Conventions – that international humanitarian law must not 'be construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations'.

International humanitarian law and the Charter of the United Nations are distinct but complementary. Concretely, the UN Charter prohibits the use of force other than in self-defence or when authorized by the UN Security Council. It also requires that international disputes be settled by peaceful means. If, however, an armed conflict breaks out, then international humanitarian law applies to set out essential protections for civilian objects and for persons who do not (civilians) or no longer (for example, wounded soldiers or detainees) participate in hostilities.

IHL does not replace or set aside the UN Charter, but rather adds a level of protection for all victims of war in the unfortunate event that a war breaks out.

See also

- Mačák and Vignati, Civilianization of digital operations: A risky trend, Asia Pacific Journal of International Humanitarian Law, 5 April 2023
- Rodenhäuser, Staehelin, Marelli, Safeguarding humanitarian organizations from digital threats, Humanitarian Law & Policy Blog, 13 October 2022
- Gisel, Rodenhäuser, Dörmann, *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts* (IRRC, 2020)
- Humanitarian Law & Policy Blog, *Human Costs of Cyber - Blog Series,* May - June 2019